Image Information Hiding: An Survey

D. Saravanan*, A. Ronald Doni** & A. Abisha Ajith***

*Assistant Professor, Department of MCA, Sathyabama University, Chennai, Tamilnadu, INDIA. E-Mail: sa_roin@yahoo.com
**Assistant Professor, Department of MCA, Sathyabama University, Chennai, Tamilnadu, INDIA. E-Mail: ronoldtony.a@gmail.com
***Student, Department of MCA, Sathyabama University, Chennai, Tamilnadu, INDIA. E-Mail: abira.mca@gmail.com

***Abstract*—**Steganography is an ancient art of hiding information to prevent the detection of hidden messages. By using this concept we proposed algorithm in this paper, to implement the concept of memory representation of sparse matrix. Sparse matrix contains the bytes of the image in which information is hidden. That means convert the image into matrix. Then convert the matrix into row matrix by find the row number, column number of none zero elements. Then choose the image which is used to hide the information object. If the output will be yes then store 0 else 1 in a matrix and this matrix will be equal to the width and height of the pixel matrix of the image. Convert the bits into bytes until all bits got utilized. Finally receiver gets the information.

***Keywords*—**Cipher Text, Information Hiding, Plain Text, Steganography, Stego Image

***Abbreviations*—**Discrete Cosine Transform (DCT), Least Significant Bit (LSB), Steganography (Stego)

I. INTRODUCTION

NOWADAYS many problems arise during the image transformation from the sender to the receiver. Strangers can easily snoop into others account and get many secret information even it was hided by some mechanism, without their permission. To avoid this we propose a secure scheme by using steganography concept. Steganography means hiding information in a particular way that prevents the detection of hidden information. In this concept no one can find that there is a hidden message present in the image, Because of information is hidden behind an image in a matrix form, which is created by bit matrix of the object. By using the LSB we can store the characteristics of particular pixels of an image are modified to store a message. Finally we send the final picture and cover image used for hidden the image to the receiver [Johnson & Jajodia, 1998].

At first we calculate the height and width of the image, which hide the information then multiply it with 8 and store it in any value. Then we calculate the height and width of the image which is used to hide the object and multiply with each other. Then we compare that answers with both the image which is used to hide the information and which is used to hide the object. The image which is used to hide the object must have greater value than the other image; we choose the object must satisfy the above condition. Then the encoded matrix is mapped with the image by using least significant bit mechanism.

Least significant bit only stores the information instead of replacing the pixel of image. So scattering of information takes place while transferring the image so according to human eye there is no difference between the original and stego image. Finally sender sends the both original and stego image to the receiver. In the receiver side to get the information the receiver must do XOR operation between bytes present in both the image. Compare the result with 0*00000000 If the output will be yes then store 0 else 1 in a matrix and this matrix will be equal to the width and height of the pixel matrix of the image. Convert the bits into bytes until all bits got utilized. Finally receiver gets the information.

1.1. History of Information Hiding

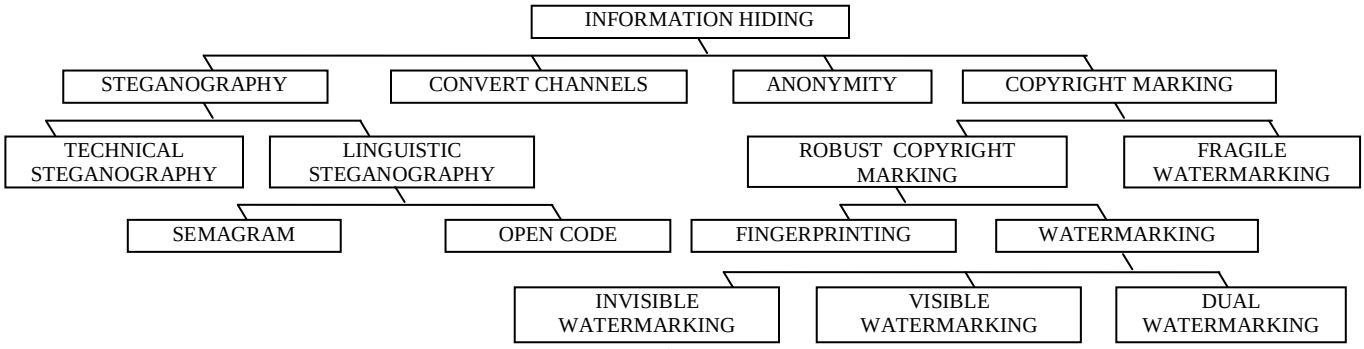

Figure 1 – Information Hiding

1.2. The Basics of Embedding

Three different aspects in information-hiding systems contend with each other: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [Fabien A. P. Petitcolas et al., 1999; Sabu M Thampi, 2004; Nameer N. EL-Emam, 2007].

1.3. Discrete Cosine Transform

For each color component, the JPEG image format uses a Discrete Cosine Transform (DCT) to transform successive 8 × 8 pixel blocks of the image into 64 DCT coefficients each. The DCT coefficients F (u, v) of an 8 × 8 block of image pixels f(x, y).

A simple pseudo-code algorithm to hide a message inside a JPEG image could look like this:

Input: message, cover image
Output: steganographic image containing message
While data left to embed do
    Get next DCT coefficient from cover image
    If DCT =! 0 and DCT =! 1 then
    Get next LSB from message
    Replace DCT LSB with message bit
End if
Insert DCT into steganographic image
End while

1.4. Detection Techniques

Many algorithms were proposed for estimating the length of the secret message in the cover image. Westfeld (2001) proposed the blind steganalysis based on statistical analysis of PoVs (pairs of values). This method, so-called statistical test, gives a successful result to a sequential LSB steganography only. Fridrich et al. proposed the RS steganalysis. This method makes small alternations to the least significance bit plane in an image the by using the following method our process [Kekre et al., 2008; Bin Li et al., 2011].

1.5. Security the Packet Decoder

The decode engine is organized around the layers of the protocol stack present in the supported data-link and TCP/IP protocol definitions. Each subroutine in the decoder imposes order on the packet data by overlaying data structures on the raw network traffic. These decoding routines are called in order through the protocol stack, from the data link layer up through the transport layer, finally ending at the application layer. Speed is highlight in this section, and the majority of the functionality of the decoder consists of setting pointers into the packet data for later analysis by the detection engine [Richard Popa, 1998].

1.6. Internet Protocol Version

Internet Protocol version 6 (IPv6) is a network layer IP standard used by electronic devices to exchange data across a packet-switched internetwork. It follows IPv4 as the second version of the Internet Protocol to be formally adopted for general use. Among the improvements brought by IPv6 is the increase of addresses for networked devices, allowing, for example, each cell phone and mobile electronic device to have its own address. IPv4 supports 4.3×10^{9} (4.3 billion) addresses, which is inadequate for giving even one address to every living person, much less support the burgeoning market for connective devices. IPv6 supports 3.4×10^{38} addresses, or 5×10^{28}(50 octillion) for each of the roughly 6.5 billion people alive today.

Normally the packets are transferred from one system to another in packets. The packets are transferred through the tcp connection in a more secure way.

II. HIDE AND SEEK: AN INTRODUCTION TO STEGANOGRAPHY

Author: Niels Provos, Peter Honeyman, Hide and Seek: Introduction to Steganography (2003).
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.3.3820

2.1. Problem Formulation

In the past, for the security purpose people used hidden tattoos or invisible ink to convey steganographic content. Today for hiding purpose computer and network technologies provide easy-to-use communication channels for steganography [Saraju P. Mohant, 2003; Muhalim Mohamed Amin et al., 2003].

Steganographic system because of their invasive nature, leave the detectable traces in the cover medium. The secret content is not revealed, but its statistical properties changed so the third party can detect the distortions in the resulting image [Morkel et al., 2005]. The process of finding the distortions is called statistical steganalysis.

2.2. Research Design

This paper explains the steganagraphic systems and presents the recent research in detecting them through statistical steganalysis.

Steganographic systems for the JPEG format seem more interesting, because the systems operate in a transform space and are not affected my visual attacks.

Visual attacks mean that we can see steganographic images on the low bit planes of an image because they overwrite the visual structures.

2.3. Finding

The JPEG image format uses a discrete cosine transform to transform successive 8*8 pixel blocks of the image into 64 DCT coefficients each.

The embedding algorithm sequentially replaces the least significant bit of DCT coefficients with the message data. The same process is also done in the JPEG format.

The author and his colleague used a support vector machine to create a nonlinear discrimination function. Then they present a less sophisticated but easier to understand method for determining a linear discrimination function.

2.4. Conclusion and Limitations

We offer four details for our inability to find steganographic content on the internet. They are,

- All steganographic system users carefully choose passwords that are not susceptible to dictionary attacks.
- May be images from sources we did not analyze carry steganographic content.
- Nobody uses steganographic systems that we could find.
- All messages are too small for our analysis to detect.

Although steganography is applicable to all data objects that contain redundancy, we consider JPEG images only for steganography.

2.5. Implications

We insert the tracer images into every stegbreak job. The dictionary attack follows the correct passwords for these images.

III. STEGANOGRAPHY AND STEGANALYSIS

Author: Robert Krenn. Steganography and Steganalysis
http://www.krenn.nl/univ/cry/steg/article.pdf

3.1. Problem Formulation

The growth of computer networks and internet has explored means of business, scientific, entertainment, and social opportunities.

The digital information can be easily duplicated and distributed has led to the need for effective copyright protection tools such as steganography and cryptography [Stefano Cacciaguerra & Stefano Ferretti, 2003; Robert Krenn, 2004].

3.2. Research Design

Secrets can be hidden inside all sorts of cover information: text, images, audio, video and more. Most steganographic utilities nowadays, hide information inside images, as this is relatively easy to implement [Christian Cachin, 1998].

Hiding information inside images is a popular technique nowadays [Shashikala Channalli, 2009]. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups.

The most common methods to make alterations in the image present in noisy area involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files.

3.3. Finding

More techniques are developed for hiding the information to detect the use of steganography. While the information can be hidden inside texts in a way that the message can only be detected with the knowledge of the secret key.

A widely used technique for image scanning involves statistical analysis, with the statistical analysis on the lsb, the difference between random values real image value can easily be detected.

The statistical analysis method can be used against the audio files too, since the lsb modification technique can be used on sounds too, including that several other things also detected.

While steganograms may not be successfully detected instead of that we use the statistical analysis from possible cover sources.

3.4. Conclusions and Limitations

Steganography combined with cryptography is a powerful tool which enables people to communicate without possible eavesdroppers even knows that there is a communication in the first place.

Steganography might also become limited laws, since government already claimed that criminals use these techniques to communicate. More restrictions are provided in the time of terrorist attacks.

3.5. Implications

In the future the most important use of steganographic techniques will lie in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials.

Although it will not prevent the distribution itself, it will enable the content provider to start legal actions against the violators of the copyrights, as they can now be tracked down.

IV. HIDING ENCRYPTED MESSAGE IN THE FEATURES OF IMAGES

Author: Kh. Manglem Singh, S. Birendra Singh & L. Shyam Sundar Singh, Hiding Encrypted Message in the Features of Images, IJCSNS, and Vol. 7, No.4, April 2007.
http://paper.ijcsns.org/07_book/200704/20070442.pdf

4.1. Problem Formulation

Steganography is the art and science of writing hidden messages in such a way that no one can't know about the intended recipient knows the existence of the message. It simply takes one piece of information and hides it with another [Kh. Manglem Singh et al., 2007].

4.2. Research Design

This process explains the least significant bit embedding algorithm for hiding encrypted messages in nonadjacent and random pixel locations in edges of images. It first encrypts the secret message and detects image in the cover image.

The simplest way to hide data on an image is to replace the least significant bits of each pixel sequentially in the scan lines across the image in raw image format with the binary data.

An attacker can easily see the message by repeating the process. To avoid this to add better security, the message to be hidden is first encrypted using the simplified data encryption standard and then it is distributed randomly by a pseudo random number generator across the image.

4.3. Finding

Many algorithms are used to estimate the length of the secret message in the cover image. Here they propose the blind steganalysis based on statistical analysis of pairs of values. This method is called statistical test.

They propose the detection algorithm based on higher order statistics for separating original images from stego images.

Blind detection algorithm that estimates the accuracy of embedded message through the analysis of the variation of the energy resultant from the lsb embedding.

4.4. Conclusions and Limitations

The paper described a novel method for embedding secret message bit in least significant bit of nonadjacent and random pixel locations in edges of images. No original cover image is required for the extraction of the secret message. It has been shown experimentally that the blind LSB detection technique like the gradient energy method could not estimate the length of the secret message bits accurately for the proposed algorithm.

4.5. Implications

The message to be hidden in the image was first encrypted using the S-DES algorithm. Then estimate the length of the secret message bits by the gradient energy technique. Gradient energy technique could not estimate the length of the secret message bit accurately.

4.6. Advantages

A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not.

Watermarking is either "visible" or "invisible". Although visible and invisible are visual terms watermarking is not limited to images, it can also be used to protect other types of multimedia object.

In steganographic communication senders and receivers agree on a steganographic system and a shared secret key that determines how a message is encoded in the cover medium. Without the key they can't identify the secret message.

In steganographic systems the images we used for hiding may be JPEG format seem more interesting because the systems operate in a transform space and are not affected by visual attacks.

4.7. Disadvantages

Encryption protects contents during the transmission of the data from the sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected.

By using the secret key we are deliver the secret message safer at the same time if any hacker finds the key then they can easily get the secret message.

Visual attacks mean that you can see steganographic messages on the low bit planes of an image because they overwrite visual structures; this usually happens in BMP images.

V. PROPOSED SYSTEM

Steganography is used to hide the information in the form of multimedia objects considering two things that is size and degree of security.

This concept assists the scattering of information at the time of hiding and implements the non traceable randomization to differentiate from the existing work.

Double embedding is done for more security.

5.1. Advantages

Steganography is the concept of hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. Here double embedding takes place. So it is safer.

It doesn't have any key to decrypt the image. So the hacker has no chance to get the message in this way.

This concept deals that the eavesdroppers will not have any suspicion that message bits are hidden in the image and standard steganography detection methods can not estimate the length of the secret message correctly.

With steganography we can send messages without anyone having knowledge of the existence of the communication.

There are many countries where it is not possible to speak as freely as it is in some more democratic countries. Then it is the easy method to send news and information without being censored and without the fear of the messages being interrupted.

5.2. Disadvantages

This concept is applied only for images not for audio and video files.

The receiver must know about the least significant bit technique.

VI. CONCLUSION

Here we conclude that we prevent the detection of hidden information by using steganography concept and propose a

secure scheme for image transformation. Here we use least significant Bit modification technique to insert the image into another image for hidden purpose. Image is hidden into another image is the technique we introduced in our paper. In other security mechanisms the strangers can easily stole the message from the image by repeating the process. But in our technique without the stego key we can't extract the message from the image. This technique facilitates the scattering of information at the time of hiding; this is new method we proposed in our paper.

VII. FUTURE ENHANCEMENT

Apart from this, any kind of future endeavor in this field will definitely route it a path to design a secure system using the proposed algorithm for both Internet and Mobile Communication Technology. The scattering of information technique is used at the time of hiding is useful for many news papers based on steganography. Development in covert communications and steganography will research in building more robust digital watermarks that can survive image manipulation and attacks. We hope some commercial and effective schemes will be available in future. In the near future, the most important use of steganographic techniques will probably lie in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials.

In future we can use this paper in the Government, Software Company, Detective agencies etc. The same step is involved to embed the information and send to particular user.

REFERENCES

[1] N.F. Johnson & S. Jajodia (1998), "Exploring Steganography: Seeing the Unseen Computer", Vol. 31, No. 2, Pp. 26–34.

[2] Richard Popa (1998), "An Analysis of Steganographic Techniques", Pp. 1–17.

[3] Christian Cachin (1998), "An Information-Theoretic Model for Steganography", *Information Hiding, Lecture Notes in Computer Science*, Vol. 1525, Pp 306-318.

[4] Fabien A. P. Petitcolas, Ross J. Anderson & Markus G. Kuhn (1999), "Information Hiding – A Survey", *Proceedings of the IEEE, Special Issue on Protection of Multimedia Content*, Vol. 87, No. 7, Pp. 1062–1078.

[5] A. Westfeld (2001), "F5-A Steganographic Algorithm: High Capacity Despite Better Steganalysis", *Proceedings of 4th International Workshop Information Hiding*, Pp. 289–302.

[6] Saraju P. Mohant (2003), "Digital Watermarking: A Tutorial Review Niels Provos, Peter Honeyman, Hide and Seek: Introduction to Steganography".

[7] Muhalim Mohamed Amin, Subariah Ibrahim, Mazleena Salleh & Mohd Rozi Katmin (2003), "Information Hiding using Steganography", Information Hiding using Steganography Approach , Vol. 71847, Pp. 1–34.

[8] Stefano Cacciaguerra & Stefano Ferretti (2003), "Data Hiding: Stegnography and Copyright Marking", *Department of Computer Science, University of Bologna, Italy*, Pp. 1–30.

[9] Robert Krenn (2004), "Steganography and Steganalysis".

[10] Sabu M Thampi (2004), "Information Hiding Techniques: A Tutorial Review", *ISTE-STTP on Network Security & Cryptography*, LBSCE 2004.

[11] T. Morkel, JHP Eloff & MS Olivier (2005), "An Overview of Image Steganography", *Proceedings of the Fifth Annual Information Security South Africa Conference(ISSA2005)*, Sandton, South Africa.

[12] Nameer N. EL-Emam (2007), "Hiding a Large Amount of Data with High Security using Steganography", *Algorithm Journal of Computer Science*, Vol. 3, No. 4, Pp. 223–232.

[13] Kh. Manglem Singh, S. Birendra Singh & L. Shyam Sundar Singh (2007), "Hiding Encrypted Message in the Features of Images", *International Journal of Computer Science and Network Security (IJCSNS)*, Vol. 7, No. 4.

[14] H.B. Kekre, Archana Athawale & Pallavi N. Halarnkar (2008), "Increased Capacity of Information Hiding in LSB's Method for Text and Image", *World Academy of Science, Engineering and Technology*, Pp. 910–913.

[15] Shashikala Channalli (2009), "Steganography: An Art of Hiding Data", *International Journal on Computer Science and Engineering*, Vol. 1, No. 3, Pp 137–141.

[16] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi (2011), "A Survey on Image Steganography and Steganalysis", *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 2, No. 2, Pp. 142–171.

D. Saravanan currently working as an Assistant Professor in the department of computer applications in Sathaybama University, Chennai. His areas of interest are image processing, data mining, DBMS. He has published paper in five national conferences & two international journals in the field of data mining.

A. Ronold Doni working as an Assistant Professor in the department of computer applications in Sathaybama University, Chennai. His areas of interest are image processing, data mining, DBMS. He has published paper in three national conferences & one international journal in the field of data mining.

A. Abisha Ajith studying First Year MCA in Sathyabama University, Chennai. Her areas of interest are image processing, data mining, DBMS. She has published paper in one national conference & one international journal in the field of data mining.